IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellants:	Cheh Goh, Liqun Chen, Stephen J. Crane, Marco C. Mont, and Keith A. Harrison		
Assignee:	Hewlett-Packard Development Company, L.P.		
Title:	Data Output Method, System and Apparatus		
Serial No.:	10/664,069	Conf. No.	3247
Examiner:	Beemnet W. Dada	Group Art Unit:	2435
Docket No.:	300110535-2	Filing Date:	September 16, 2003

December 30, 2009

Mail Stop APPEAL BRIEF - PATENTS
COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

CORRECTION OF APPEAL BRIEF UNDER 37 C.F.R. §§ 1.191 AND 41.67

Dear Sir:

Appellants submitted an Appeal Brief in the above-identified patent application on November 16, 2009, pursuant to the Notice of Appeal filed on September 16, 2009. The Notification of Non-Compliant Appeal Brief dated December 3, 2009 indicated that the "V. Summary of Claimed Subject Matter" was not in compliance with 37 CFR 41.37(c)(1)(v). Appellants' description of the claimed subject matter referred to paragraph numbers that were used in the published application. Appellants are replacing the originally filed section V in the Appeal Brief filed November 16, 2009 with the section V below, which contains references to page and line numbers in the original specification submitted on September 16, 2003.

The Notification dated December 3, 2009 under box 10 also refers to "section IV." Appellants believe that this was a typographical error and that "section V" was intended. However, sections IV and V are provided below.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

IV. STATUS OF AMENDMENTS

There are no unentered amendments in this case. No amendments were filed subsequent to the final rejection dated June 16, 2009.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The present invention relates to protection of information that might be output to a removable medium. For example, some embodiments of the invention implement security policies for printing of information. Embodiments of the invention can employ Identifier Based Encryption (IBE) using a representation of a security policy as the identifier string in the IBE that encrypts the information to be protected from unauthorized output. An output device then needs a decryption key before the information can be decrypted and output in unencrypted or plain text form. These embodiments can reduce or avoid the chance of a security breach that might result from a malicious attempt to provide altered security policy information to a trusted authority that can provide a key for decrypting the information. In particular, the trusted authority must be provided with the correct policy information in order to generate the correct decryption key. Accordingly, the trusted authority can check compliance with the correct security policy before providing a decryption key.

Independent claim 1 is directed to a system such as illustrated in Fig. 3 including: "an output device for outputting data onto a removable storage medium," e.g., printer 30; "a first computing entity for encrypting a first data set," e.g., the user's computing entity 20; and "a second computing entity associated with the trusted party," e.g., computing entity 21.

The first computing entity 30 encrypts the first data set, e.g., encrypts a document to be printed as described in page 8, lines 1-4. The parameters used in the encryption includes: "public data of a trusted party," e.g., a public key *R*, and "an encryption key string comprising a second data set that defines a policy for allowing the output of the first data set onto a said removable storage medium," e.g., string *ID*. Page 8, lines 1-4 describes how computing entity 20 can encrypt a document for printing using a representation of the policy as an encryption key string in an IBE (Identifier-Based Encryption) process. Page 9, line 12 to page 11, line 19 describe an IBE process in detail. Page 10, lines 24-27 particularly describes encryption using an identifier based public key Q_{ID}/private key S_{ID} pair, where $S_{ID}=sQ_{ID}$, s is a secret of the trusted authority, and Q_{ID} is the public key for identifier string ID that represents the policy for printing the encrypted document. The first computing entity is "further arranged to output the encrypted first data set for the output device," e.g., entity 20 forwards the cipher text to printer 30 as described in page 8, lines 6-8.

The second computing entity 21 is "arranged when satisfied that said policy has been met, to output for the output device a decryption key, distinct from the encryption key string,

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

for use in decrypting the encrypted first data set," as described in page 9, lines 1-10. The second computing entity is "arranged to generate this decryption key in dependence on the encryption key string and private data related to said public data." A decryption key S_{print} as described in page 11, lines 25-30 depends on the public key $Q_{print}=Q_{ID}$ and therefore depends on the encryption key string ID. Claim 1 finishes by reciting, "the output device being arranged to use the decryption key in decrypting the encrypted first data set" as described in page 8, lines 16-21.

Independent claim 15 is directed to a data output method that includes, "(a) encrypting a first data set," e.g., encrypting a document for printing as described in page 8, lines 1-4. The encrypting is "based on encryption parameters that comprise: i. public data of a trusted party, and ii. an encryption key string comprising a second data set that defines a policy for allowing the output of the first data set to a removable storage medium." The public and private data of an identifier based encryption process is described in page 9, line 12 to page 11, line 19, and use the policy, or a representation of the policy, as an encryption key string in an IBE as described in page 8, lines 1-4. Step (b), "providing the encrypted first data set to an output device adapted to output data to a removable storage medium," corresponds in the embodiment illustrated in Fig. 3 to a user's computing entity 20 providing encrypted data to a printer 30 as described in page 8, lines 6-8. Step (c), "at the trusted party checking that said policy has been satisfied and thereafter providing the output device with a decryption key, distinct from the encryption key string, for use in decrypting the encrypted first data set, this decryption key being generated in dependence on the encryption key string and private data related to said public data" corresponds in the embodiment of Fig. 3 to trust authority computing entity 21 checking for compliance with the policy as described in page 9, lines 1-10 and generating a decryption key, for example, as described in page 11, lines 25-30. Final step (d), "at the output device using the decryption key in decrypting the encrypted first data set and outputting the first data set to a removable recording medium" is described in page 9, lines 1-10 in regard to the decrypting and printing of a document.

Independent claim 28 is specifically directed to a printing system. For example, the printing system illustrated in Fig. 3 includes: "a printer" e.g., printer 30; "a first computing entity for encrypting a first data set," e.g., computing entity 20; and "a second computing entity associated with the trusted party," e.g., computing entity 21. The first computing entity encrypts the first data set based on encryption parameters that comprise: i. public data of a trusted party, and ii. an encryption key string comprising a second data set that defines a

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

policy for allowing the printing of the first data set. See paragraphs page 9, line 12 to page 11, line 19. The first computing entity is further arranged to output the encrypted first data set for the printer as described in page 8, lines 6-8, The second computing entity is "arranged when satisfied that said policy has been met, to output for the printer a decryption key, distinct from the encryption key string, for use in decrypting the encrypted first data set, the second computing entity being arranged to generate this decryption key in dependence on the encryption key string and private data related to said public data." See page 9, lines 1-10 and page 11, lines 25-30 as noted above. Finally, "the printer being arranged to use the decryption key in decrypting the encrypted first data set" is described in page 9, lines 1-10.

Please contact the undersigned attorney at (530) 621-4545 if there are any questions concerning the Appeal Brief or the application generally.

Respectfully submitted,

/David Millers 37396/

David Millers
Reg. No. 37,396

PATENT LAW OFFICE OF DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543